CLAIM LISTING

Please amend claim 6, add claims 21 to 26, and cancel claims 1 to 5 as indicated below.

1. (Canceled)

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. (Canceled)

6. (Currently amended) A method for automated detection of monitoring data sources of at least one remotely located computer system in a network environment, said method comprising ~~the steps of~~:

providing a configuration containing instructions that query at least one of said at least one remotely located computer system, said configuration comprising a service table identifying one or more services provided by the remotely located computer systems ~~that are usable~~ to monitor said at least one computer system, the services being non-monitoring specific and the remotely located computer systems absent the monitoring computer program, a detection table identifying information to detect at least one of the monitoring data sources, and a metric table identifying a metric for the at least one of the monitoring data sources;

providing a data detection module configured to generate multiple service probe requests to detect configured to identify different services at two or more remotely-located computer systems that are unidentified;

identifying, by said data detection module using said configuration, accessible data sources of at least one of said at least one computer system, the accessible data sources being different from that at another computer system;

using subsets of metric probe requests to collect ~~collecting~~ from at least one of said computer systems meta and performance information of said accessible data sources of at least one of said at least one computer system, the meta and performance information comprising a response from at least one of the services provided by the remotely located computers systems, whereby one subset of the metric probe requests is based on identification of the at least one of the services and another subset of the metric probe requests is based on identification of another one of the services;

~~embedding an expert's knowledge concerning monitoring information services into a monitoring configuration in software used to automate said step of collecting meta and performance information;~~

presenting said meta and performance information to a user; and

presenting a list of said identified accessible data sources to said user, wherein said list of said identified accessible data sources is derived using the different services.

7. (Original) The method according to claim 6, further comprising the step of:

receiving access information from said user, wherein said access information comprises one member of the group consisting of a username and a password.

8. (Original) The method according to claim 6, further comprising the steps of:

receiving a list of data sources chosen by said user;

extracting said meta and performance data from said chosen data sources; and

presenting said meta and performance data to said user.

9. (Previously presented) The method according to claim 6, further comprising the step of:

utilizing a probe engine to verify whether a service of one of said at least one computer system is responding, and

determining, said meta and performance data of an environment in which said service is running, in response to said probe engine verifying said service is running.

10. (Original) The method according to claim 9, wherein the service probing step is performed for each service of said at least one computer system.

11. (Previously presented) The method according to claim 9, further comprising the steps of:

utilizing said probe engine to identify at least one monitoring information source in said at least one computer system, and

storing said monitoring information source in a list of said at least one identified monitoring information sources.

12. (Previously presented) The method according to claim 11, wherein the monitoring information source probing step utilizes the probe engine to identify the monitoring information source and storing the monitoring information source in the list of detected monitoring information sources are performed for each monitoring information source of said at least one computer system.

13. (Original) The method according to claim 11, further comprising the step of:

utilizing said probe engine to determine a metric associated with each of said monitoring information sources.

14. (Original) The method according to claim 6, wherein said meta information comprises set-up information of said at least one computer system.

15. (Canceled).

16. (Previously presented) The method according to claim 8, wherein said list receiving step comprises receiving a range of data sources of said network environment, said range being specified by said user.

17. (Canceled)

18. (Canceled)

19. (Previously presented) The method according to claim 6, wherein each of said services identified in said service table are associated with a service type, the method further comprising the step of activating a probe engine according to at least one service type, wherein the probe engine probes a monitoring information service to monitor information of the computer system.

20. (Previously presented) The method according to claim 6, wherein the step of collecting meta and performance information further comprises populating the list of the accessible data sources, wherein the list of the accessible data sources is initially empty.

21. (New) An apparatus for detecting and monitoring data sources, the apparatus comprising:

a computer having a processor and a memory configured to receive monitoring information from one or more remotely-located computer systems, the monitoring information concerning the operation of the one or more remotely-located computer systems; and

a computer-readable medium encoded with executable instructions configured to instruct the computer to:

implement probe engines to generate probe requests that detect services, at least two probe engines being configured to identify different services at the one or more remotely-located computer systems that are unidentified;

transmit a first set of service probe requests and a second set of service probe requests via a network to detect whether a first service and a second service, respectively, are associated with the remotely-located computer systems;

identify that the first service and the second service are available at a first remotely-located computer system and a second remotely-located computer system, respectively;

transmit a first set of metric probe requests and a second set of metric probe requests to the first service and the second service, respectively, to determine a first set of metrics and a second set of metrics, the transmission of the first set of metric probe requests and a second set of metric probe requests is based on responses generated by the first set of service probe requests and the second set of service probe requests; and

generate data to present representation of the first set of metrics and the second set of metrics via a graphical user interface.

22. (New) The apparatus of claim 21, wherein the first service and the second service are different services.

23. (New) The apparatus of claim 21, wherein at least one metric probe request from both the first set of metric probe requests and the second set of metric probe requests is transmitted to both the first service and the second service.

24. (New) The apparatus of claim 21, wherein the computer-readable medium encoded with executables instructions further comprises executable instructions to:

transmit sets of service probe requests including the first set of service probe requests and the second set of service probe requests to detect services in the remotely-located computer systems;

transmit a number of monitoring information source ("MIS") probe requests for each of the services that causes responses to the sets of service probe to detect a subset of MISs; and

associate each MIS of the subset of MISs with one of the services to form an association that is stored in a MIS detectable table,

wherein the MIS detectable table includes data from different services.

25. (New) The apparatus of claim 24, wherein the computer-readable medium encoded with executables instructions further comprises executable instructions to:

transmit sets of metric probe requests for each of the MISs that causes a response to the number of MIS probe requests, the sets of metric probe requests including the first set of metric probe requests and the second set of metric probe requests to detect metrics in the remotely-located computer systems;

detect a subset of metrics; and

associate each metric of the subset of metrics with one of the MISs to form an association that is stored in a metric table,

wherein the MIS detectable table includes data from the different services, wherein the first set of metric probe requests is a function of the first set of service probe requests and the second set of metric probe requests is a function of the second set of service probe requests.

26. (New) The apparatus of claim 21, wherein the computer-readable medium encoded with executables instructions configured to identify that the first service and the second service are available for the first remotely-located computer system and the second remotely-located computer system, respectively, comprises executable instructions to:

determine that one of the first service and the second service is a command line-based service; and

determine that other of the first service and the second service is a graphical user interface ("GUI")-based service.